AO 106A (EDVA Version) (03/20) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
IN MATTER OF SEARCH OF INFORMATION ASSOCIATED WITH 8 GMAIL ACCOUNTS DESCRIBED IN ATTACHMENT A

Case No. UNDER SEAL 3:21SW 49

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A to Affidavit, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B to Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1349	Conspiracy and Attempt to Commit Wire Fraud
18 U.S.C. § 1956(h)	Conspiracy to Commit Money Laundering

The application is based on these facts:

See Attached Affidavit.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Steele D. Holland
Applicant's signature

Reviewed by AUSA/SAUSA
Shea Gibbons
Printed name and title

Steele Holland, TFO, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: April 14, 2021

/s/ GMA
Judge's signature

City and state: Richmond, Virginia

Elizabeth W. Hanes
United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH EIGHT (8) GMAIL ACCOUNTS DESCRIBED IN ATTACHMENT A, THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 3:21SW49 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Steele Holland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC (hereafter "Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Task Force Officer of the Federal Bureau of Investigation (FBI) assigned to the Richmond Division and detailed from the Virginia Department of State Police. I became a Task Force Officer with the FBI in March 2015. I am currently assigned to the Cyber Squad

within the Richmond Division where I am primarily responsible for the investigation of cyber matters, which include computer-enabled criminal violations relating to computer-enabled fraud designed to induce victims to wire money to criminally controlled bank accounts. Before becoming a Task Force Officer, I was assigned as a Special Agent with the Virginia Department of State Police starting in January 2014. In that role, I received and distributed intelligence material to appropriate parties and provided field support by way of actionable intelligence. Prior to my role as a Special Agent, I was a uniformed state trooper with the Virginia Department of State Police, beginning in January 2003. Throughout my employment as a police officer, I conducted criminal investigations and I have received many classes in basic and advanced criminal investigation techniques. As a Task Force Officer with the FBI, I have received training in the investigation of cases involving computer crimes and the use of computers to advance criminal schemes.

3. As a Task Force Officer of the FBI, I am authorized to conduct investigations, carry firearms, execute warrants, make arrests for offenses against the United States and perform other such duties as are authorized by the FBI. Through the course of these investigations, I have conducted interviews and secured other relevant information using a variety of investigative techniques.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of federal criminal law, specifically wire fraud

(18 U.S.C. § 1343); conspiracy and attempt to commit wire fraud (18 U.S.C. § 1349); and money laundering conspiracy (18 U.S.C. § 1956(h)), have been committed by the person in control of the following email addresses:

- **lwestendtoys@gmail.com (Target Account No. 1),**
- **seller-performance@8cnzvfen-amazon.com (Target Account No. 2),**
- **seller-performance@2bv5bden-amazon.com (Target Account No. 3),**
- **seller-performance@1cr4x7en-amazon.com (Target Account No. 4),**
- **edelmira.salinas.ruiz@gmail.com (Target Account No. 5),**
- **mata82465@gmail.com (Target Account No. 6),**
- **detreaba112@gmail.com (Target Account No. 7), and**
- **adypv1@gmail.com (Target Account No. 8).**

There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

7. Title 18, United States Code, Section 1343 (wire fraud) provides:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any

> writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

8. Conspiracy to commit wire fraud, as set forth in 18 U.S.C. § 1349, provides in pertinent part:

> Any person who attempts or conspires to commit [wire fraud] shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

9. Money laundering as set forth in 18 U.S.C. §§ 1956(a) is described in pertinent part as follows:

> (a)(1) Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—
>
> (A)(i) with the intent to promote the carrying on of specified unlawful activity; *or*
>
> * * *
>
> (b) knowing that the transaction is designed in whole or in part—
>
> (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity;
>
> * * *
>
> shall be sentenced to a fine of not more than $500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.

10. Title 18, United States Code, Section 1956(h) provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

11. **Specified Unlawful Activity:** The definition of "specified unlawful activity" is given in 18 U.S.C. § 1956(c)(7), which lists several categories of offenses that constitute

"specified unlawful activity." Wire fraud, penalized under 18 U.S.C. § 1343, is included as a "specified unlawful activity" for purposes of money laundering in 18 U.S.C. § 1956(c)(7)(A), which in turn incorporates the list of "racketeering activities" set forth in 18 U.S.C. § 1961(1).

PROBABLE CAUSE

12. The United States is investigating the unauthorized access of Amazon seller accounts and subsequent changing of the associated banking information, resulting in Amazon disbursements to those sellers being redirected to foreign bank accounts. This fraud happened in two stages. In the first stage of this fraud, subjects conducted a phishing campaign, where they used Gmail accounts to spoof Amazon emails. These phishing emails were designed to compromise the login credentials of Amazon sellers. In the second stage, the subjects used Amazon Web Services (AWS) accounts to log in to the seller accounts and to change the seller's disbursement bank account to a foreign bank account controlled by the subjects. Several of the AWS accounts established and used by the subjects had Gmail addresses associated with them.

Amazon Background

13. Amazon is an online retailer headquartered in Seattle, Washington. Among other businesses, Amazon runs widely known e-commerce websites. Amazon calls these websites "stores." Amazon offers products for sale in its stores that are sold by Amazon itself, and products that are sold by third-party sellers.

14. Each third-party seller must create a unique account with Amazon. To create a third-party seller account, users must provide Amazon with a variety of information and documentation, including a government-issued ID, tax information, and a phone number. Sellers must also provide a financial account so that Amazon may disburse funds owed to the seller through sales made on Amazon's stores. A seller may update this financial account at any time.

Sellers are able to use virtual bank accounts through companies like Hyperwallet, which, among other things, facilitate currency transfers not otherwise supported by Amazon. Approximately every 14 days, Amazon disburses funds from the third-party seller's Amazon account to the seller's account on file.

15. Amazon also operates the subsidiary Amazon Web Services, Inc. ("AWS"), which provides cloud computing services, including Amazon Elastic Compute Cloud ("EC2"), a scalable service that allows users to rent virtual computers on which to run computer applications. Each AWS customer must create a unique account with Amazon by providing Amazon with information, including an email address, phone number, and payment method.

Initial Complaint

16. On November 24, 2020, Evans Richards, Owner and CEO of West End Toys, LLC, an online toy seller based in Richmond, determined that the company's Amazon account was compromised and that a bi-weekly payment was redirected to an unknown bank account ending in 629. However, Amazon was later able to stop the disbursement and return the funds to West End Toys, LLC. The attempted losses due to the fraud were $176,469.62.

17. Richards advised that a week prior, West End Toys had received a phishing message and that one of his employees had responded and provided the company's telephone number associated with its Amazon account. Additionally, this employee received a second message and clicked on a hypertext "button" contained in it. This message was sent from IP address 74.208.4.194.

18. On November 24, 2020, Amazon provided the following information regarding the bank account to which the subjects attempted to redirect the funds:

- Routing number: 073972181

- Account number: 4452757076629

19. In examining the West End Toys account's sign-in history, Amazon determined that West End Toys' account was accessed on November 17, 2020. After this access, the email address on the account was changed to **lwestendtoys@gmail.com (Target Account No. 1)**, which added an "l" to the beginning of the email address already on the account. The bank account was also updated to the account ending in 629, which was the destination for the fraudulent disbursement cancelled on November 24, 2020.

How the West End Toys Account was Compromised

20. West End Toys received two emails on November 17, 2020, sent to their westendtoys@gmail.com address. In the first message, allegedly sent by Seller Notification, seller-notification@www-amazon.com, they were informed that Amazon was unable to verify some of the information in their seller account. These emails instructed West End Toys to log into their Amazon Seller Central account, locate the emergency notification section, and to enter a valid phone number. Once this was completed, they were to reply within 24 hours with a confirmation email and they would be sent a verification email to confirm the update as the principal account owner. A review of the message header revealed that the Reply-To address was **seller-performance@8cnzvfen-amazon.com (Target Account No. 2)**.

21. A few minutes later, West End Toys received a message that appeared to be from seller-performance@amazon.com, with the actual address being **seller-performance@8cnzvfen-amazon.com (Target Account No. 2)**. A Whois query for this domain at Centralops.net revealed that the mail exchange (MX) records resolved to Google.com (in other words, an email account associated with Google). This message thanked West End Toys for their confirmation email and instructed them to click on a "Complete Review" button in the email to

confirm the update of their phone number as principal account owner. This button contained a hyperlink that connected to https://www.google.com/url?q=https://sellercentral.amazn.com-594040.eu/ap/en/view?c3e72d83-9e52-442d-8c73-376ad760aff9&sa=D&sntz=1&usg=AFQjCNGgeM1cmh22ib3LZaXlsjhYnCU5fQ. These messages were received and the "Complete Review" button was clicked on by West End Toy's employee Michael D. Jones.

22. On November 26, 2020, November 30, 2020, and December 1, 2020, West End Toys received three additional emails. Each of these was sent as a reply to the confirmation email Jones had sent to the original phishing message confirming their phone number. These messages appeared to be from either Seller Notification or seller-performance@amazon.com, but each actually came from **seller-performance@8cnzvfen-amazon.com (Target Account No. 2)**. Additionally, the content of these emails was similar, with each claiming an issue had been found with West End Toys' seller account that needed to be addressed immediately and including a "Fix Issue" button. The hyperlink for each of these buttons was directed to https://www.google.com/url?q=https://sellercentral.amazn.com-492950.eu/ap/en/view?df0de9d4-0954-4962-b1af-66358eb64805&sa=D&sntz=1&usg=AFQjCNHL3-HT8ubN-Oc-cdal6EM2pC-P1w.

23. On December 2, 2020, FBI agents examined the laptop computer on which Jones clicked the link in the second email and conducted a memory capture. A review of this memory capture did not identify any indicators for the presence of malware. On December 15, 2020, Richmond Division's Computer Scientist opened the second email received by West End Toys and clicked on the "Complete Review" button and was redirected to https://sellercentral.amazon.com-f3xy8od3.eu. This website had the appearance of Amazon

Seller Central and included a login prompt. When false login information was entered, a confirmation prompt was displayed asking that the login information be reentered, with an additional CAPTCHA.

Resale Addict Account Compromise

24. Based upon information provided by Amazon, FBI agents contacted and interviewed Heath Harris, the owner of a business named Resale Addict, and a victim of a similar scheme to that suffered by West End Toys. Resale Addict's loss was $8,491.33. On October 29, 2020, Harris received an email to his resaleaddict1@gmail.com email address from Seller Notification, **seller-performance@2bv5bden-amazon.com (Target Account No. 3)**. This email was very similar in content to the first email received by West End Toys, requesting the input of a valid phone number and a confirmation reply message. After Harris responded, he received a second email on October 29, 2020 from **seller-notification@2bv5bded-amazon.com (Target Account No. 3)**, requesting that he verify his recent account changes by clicking on a "Begin Verification" button. Harris advised that he clicked on this link. A Whois query for this domain at Centralops.net revealed that the mail exchange (MX) records associated with **seller-notification@2bv5bded-amazon.com (Target Account No. 3)**, resolved to Google.com (in other words, an email account associated with Google). The "Begin Verification" button contained a hyperlink to https://www.google.com/url?q=https://sellercentral.amazn.com-095890.eu/ap/en/view?b8fec1c1-1700-445d-a367-60d1cf18fc2a&sa=D&sntz=1&usg=AFQjCNEWDxIrxHYeHppZbpdWNWEIzmheYA.

25. On December 10, December 17, and December 22, 2020, Harris received three additional emails from the subjects. Each of these messages indicated that an issue had been found with Resale Addict's Amazon Seller Central account and requested a reply to start the

verification process. The contents of these messages were similar to the first emails received by both Resale Addict and West End Toys and did not include buttons with hyperlinks. The December 10, 2020 and December 17, 2020 messages were allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To addresses for each was **seller-performance@1cr4x7en-amazon.com (Target Account No. 4)**. A Whois query at centralops.net of the **1cr4x7en-amazon.com** domain revealed MX records associated with Google.com (in other words, an email account associated with Google). The December 22, 2020 email was also allegedly sent from Seller-Notification, seller-notification@www-amazon.com, but the Reply-To address was **seller-performance@8cnzvfen-amazon.com (Target Account No. 2),** the same email address used for messages received by West End Toys.

Potential Related Seller Account Takeovers and Disbursements

26. Using the West End Toys account, Amazon identified certain attributes by which it could identify potentially related incidents. Those data points included: (1) IP access from IP ranges 104.128.112.0 – 104.128.127.255 and 154.13.53.0 - 154.13.63.2552; (2) target URLs that would allow the perpetrators to change email settings and view upcoming disbursements; and (3) account access from a new device.

27. From that work, Amazon identified 622 accounts that contained those attributes between late August and December of 2020. Based upon their investigation to date, Amazon deemed it likely that the perpetrators accessed each of these 622 accounts. Of these accounts, 267 had their financial accounts changed after the malicious access. The activity on these identified accounts followed a similar pattern to what occurred on the West End Toys account. The perpetrators first accessed the seller's account from one of the IP ranges identified above. The perpetrators then visited the seller's account notification section and changed the email

address used for account update notifications, often providing a new address that added an "l" to the beginning of the existing address on the account (e.g., **lwestendtoys@gmail.com (Target Account No. 1)**). The perpetrators also accessed the disbursement page, which details the amount and timing of any upcoming disbursements. Ultimately, the perpetrators changed the designated financial account for disbursements so that any future disbursements were paid to the subjects' financial account.

28. Of the 267 accounts where the financial account was changed, the perpetrators obtained $529,834.90 (USD) in fraudulent disbursements. The perpetrators also attempted fraudulent disbursements totaling $2,208,444.92 (USD), $576,138.47 (Mexican Pesos) and $26,662.88 (Canadian Dollars). However, Amazon's controls identified these latter attempted disbursements as potentially fraudulent and canceled them.

29. In January 2021, Amazon provided information on several of the merchants whose accounts were compromised during November 2020, including West End Toys. Similar to West End Toys, the disbursement bank account information for these sellers was changed by the subjects to routing number 073972181 and account numbers beginning with 445. This routing number corresponds to MetaBank. However, further investigation revealed that the disbursements were made through Hyperwallet, a third-party payment service provider formerly owned by MetaBank. Sellercentral.amazon.com allows merchants to use Hyperwallet as one option to make global payments. The Amazon Hyperwallet Getting Started Guide, located at sellers.hyperwallet.com/tmp/files/1871789/Getting%20Started%20Guide.pdf, details how an Amazon seller sets up and uses a Hyperwallet account. This document describes how, when creating their Hyperwallet account, a merchant enters their banking details and a Deposit Account is automatically generated. Further, these instructions include an image showing an

example of a generated deposit account with routing number 073972181 and an account number beginning with 445 (i.e., 4454847652867).

30. When asked, Hyperwallet representatives confirmed that a proxy account, called a Deposit Account, was generated by sellers using the amazon.hyperwallet.com system. These Deposit Accounts appear to Amazon to be U.S.-based accounts but in fact were merely used here to forward any funds deposited in them to foreign bank accounts. These Deposit Account numbers were the account numbers beginning with 445 entered by the subjects into the compromised Amazon merchant accounts. In sum, the subjects used Hyperwallet accounts, appearing as U.S.-based accounts to Amazon, to transmit the rerouted funds from hijacked Amazon seller accounts to foreign bank accounts.

31. The data provided by Amazon documented those merchants where the account compromise resulted in a successful disbursement to one of the subjects' accounts and those where the disbursement was cancelled or unsuccessful. Based upon signature IDs for successful transfers and the proxy Hyperwallet Deposit Account numbers, Hyperwallet was able to provide information on the foreign bank accounts associated with each of these Deposit Accounts. The vast majority of the foreign bank accounts were located in Romania, with a substantial amount in Greece, and a few in Hungary.

Subjects' AWS Account Information

32. In reviewing the account activity described above, Amazon discovered that the perpetrators often accessed and made changes to the seller accounts from AWS-hosted EC2 virtual machines. Each EC2 "instance" (i.e., a virtual machine akin to logging into and using a computer remotely) is associated with an AWS account. In many of those cases, subjects would make changes to the seller accounts, including updating financial account information, from the

AWS services. The below sections provide details on the subjects' AWS accounts identified to date, many of which were closed for non-payment. Amazon has preserved network traffic and 121 instances connected to AWS accounts 619554062742 and 169587936196.

33. Much of the subjects' recent AWS activity was traced to AWS account 619554062742, which was opened on October 20, 2020. Amazon provided the following information for this account:

AWS Account: 619554062742 (AWS Account No. 1)
Email: roxanac2020@protonmail.com
Registered Name: roxanac2020
Account registered on: 10/20/2020
Account closed on: 01/26/2021
Phone: +40 757297823 (RO)
Billing address: RO, Ilfov, Magurele, Alunis 59, 077125, Romania
Debit cards:

- 4256031149608984, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 4256031155538935, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 5275294800107845, account holder SANDU ROXANA COSTINA, issued by OTP Bank Romania S.A

34. According to Amazon, the subjects using AWS Account No. 1 launched 397 separate EC2 low compute capacity instances with Microsoft Windows operating systems (i.e., virtual Windows machines) and used those instances to access the Amazon seller accounts at issue. For example, the seller account 5738863805, for Resale Addict, 14325 Fox Knoll Dr., Colonial Heights, VA 23834, was accessed from IP 154.13.62.141 (within one of the subjects' attacking IP ranges) on October 30, 2020. After that date, the account was accessed numerous

times from AWS Account No. 1. Ultimately, the subjects obtained a fraudulent disbursement of $8,491.33 on November 10, 2020.

35. The subjects generally connected to AWS Account No. 1 from IP addresses associated with known VPN services. However, some December 2020 and January 2021 connections were made from IP address 185.53.199.131, which public records associate with a Romanian ISP provider, Orange Romania S.A.

36. On January 4, 2021, the subjects registered AWS account 169587936196 with the name "roxanacostina22." This account shared a debit card and billing address with the AWS Account No. 1 described above. This account was also accessed from IP address 185.53.199.131. The complete customer details are below:

AWS Account: 169587936196 (AWS Account No. 2)
Email: roxanacostina22@protonmail.com
Registered Name: roxanacostina22
Account registered on: 01/04/2021
Phone: +40 755397643 (RO)
Billing address: RO, Ilfov, Magurele, Alunis 59, 077125, Romania
Debit cards:

- 5275294800107845, account holder ROXANA COSTINA, issued by OTP Bank Romania S.A

37. Using data for AWS Accounts No. 1 and No. 2, Amazon identified nine other AWS accounts that were likely controlled by the same individuals, but three of the nine AWS accounts did not have an associated Gmail address, or linked to another account with an associated Gmail address, and so are not included in this warrant related to Gmail addresses. These accounts are connected by the same debit cards, card holder names, phone numbers, and/or billing addresses. These accounts were also used to launch at least 806 EC2 low compute

capacity instances with Microsoft Windows operating systems between December 11, 2019 and October 23, 2020. Below are the customer details for these accounts.

AWS Account: 723015188175 (AWS Account No. 3)
Email: ROXANACOSTINA@protonmail.com
Registered name: ROXANACOSTINA
Account registered on: 09/09/2020
Account closed on: 11/11/2020
Phone: +40 727571425
Billing address: RO, Ilfov, Magurele, Alunis 59, ZIP 077125, Romania
Debit cards:

- 4256031149608984, account holder SANDU ROXANA COSTINA, issued by ING Bank N.V. Romania
- 4256031171828138, account holder PAVEL DANIEL, issued by ING Bank N.V. Romania

AWS Account: 381237994080 (AWS Account No. 4)
Email: mata82465@hotmail.com:
Registered name: mata82465
Account registered on: 11/10/2020
Account closed on: 11/10/2020
Phone: +44 7496283668
Billing address: GB, Glasgow Lanarkshire 17 Finlay Drive G31 2BD, United Kingdom
Debit cards:

- 4256031171828138, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania
- 4256031180393017, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania
- 4256031155538935, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania

- 4256031149608984, account holder SCOTT WALKER LYONS, issued by ING Bank N.V. Romania

AWS Account: 828411491198 (AWS Account No. 5)
Email: **edelmira.salinas.ruiz@gmail.com (Target Account No. 5)**
Registered name: edelmira2020
Account registered on: 09/02/2020
Account closed on: 09/16/2020
Phone: +40 729767365
Billing address: GB, Beverley, East Yorkshire, 128 Flemingate, 077125, United Kingdom
Debit cards:

- 4256031180393017, account holder EDELMIRA SALINAS RUIZ, issued by ING Bank N.V. Romania
- 5374340007628891, account holder EDELMIRA SALINAS RUIZ, issuing bank unknown.

AWS Account: 084088975645 (AWS Account No. 6)
Email: **mata82465@gmail.com (Target Account No. 6)**
Registered name: mata82465
Account registered on: 06/24/2020
Account closed on: 07/12/2020
Phone: +40 723721483
Billing address: RO, Bucharest, Strada Nufarul Galben 89, 077120, Romania
Debit cards:

- 4026430050767772, account holder 190, issuing bank unknown.
- 5374340007628891, account holder EDELMIRA SALINAS RUIZ, issuing bank unknown.

AWS Account: 336612857999 (AWS Account No. 7)

Email: **detreaba112@gmail.com (Target Account No. 7)**

Registered name: Pavel Daniel

Account registered on: 11/12/2019

Account closed on: 11/11/2020

Phone: +40 752762035

Billing address: RO, Jilava, Str. Toamnei Nr. 28, 077120, Romania

Debit cards:

- 4256031171828138, account holder PAVEL DANIEL, issued by ING Bank N.V.
- 4256031169811781, account holder MANDA SANDEL, issued by ING Bank N.V.
- 4462951002519350, account holder PAVEL DANIEL, issued by Unicredit Tiriac Bank S.A.
- 4462951002427281, account holder VARIA IONUT MARIAN, issued by Unicredit Tiriac Bank S.A.
- 4462951002035928, account holder FLORIAN GHITA, issued by Unicredit Tiriac Bank S.A.

AWS Account: 890661272750 (AWS Account No. 8)

Email: **adypv1@gmail.com (Target Account No. 8)**

Registered name: adypv1

Account registered on: 07/30/2020

Account closed on: 08/15/2020

Phone: +40 727571425

Billing address: RO, Bucharest, Nufarul Galben 89, 077120, Romania

Debit cards:

- 4026430050767772, account holder EDELMIRA SALINAS RUIZL, issuing bank unknown.
- 4256031180393017, account holder NIDELEA DRAGOS, issuing bank unknown.

Relationship of Target Email Accounts to Reported Fraud

38. As mentioned above, Amazon discovered that the perpetrators often made changes to the compromised seller accounts using AWS Account No. 1. Amazon determined that AWS Account No. 2 was being used to conduct additional continuing fraud. A review of the details of these two accounts revealed that they had similar registered names (roxanac2020 and roxanacostina22), similar email addresses (roxanac202@protonmail.com and roxanacostina22@protonmail.com), and shared the same billing address. In addition, both AWS Accounts No. 1 and No. 2 were associated with debit card account number 5275294800107845, with the former listing the account holder as Sandu Roxana Costina and the latter as Roxana Costina.

39. Amazon also identified other AWS accounts they believed were likely controlled by the same perpetrators, based upon common elements in their registration data. While the AWS accounts using **Target Accounts No. 5 to No. 8** do not have any direct connections to the registration data for AWS Accounts No. 1 and No 2, they have common elements with AWS Accounts No. 3 and No 4, which in turn share elements with the first two AWS accounts. As described above, Amazon Sellers have been targeted over a period of time, with the subjects creating new email addresses and AWS accounts as needed to support their fraudulent activities. These accounts are able to be associated by highlighting the singular or multiple links of common identifiers that were reused and shared when creating additional accounts.

40. **Target Account No. 5** was the email address for AWS Account No. 5. AWS Account No. 5 includes debit card 4256031180393017, which was also associated with AWS Account No. 4. AWS Account No. 4 also includes debit card numbers 4256031155538935 and

4256031149608984, which were also associated with AWS Account No. 1, the main AWS account used to perpetrate this aspect of the fraud scheme.

41. **Target Account No. 6** was the email address for AWS Account No. 6. The account data for AWS Account No. 6 includes debit card 5374340007628891, which was also included as a debit card for AWS Account No. 5. As shown in the preceding paragraph, AWS Account No. 5 can be linked first to AWS Account No. 4 and then to AWS Account No. 1.

42. **Target Account No. 7** was the email address for AWS Account No. 7. AWS Account No. 7 includes debit card number 4256031171828138, which was also associated with AWS Accounts No. 3 and No. 4. While the link from AWS Account No. 4 to AWS Account No. 1 has already been shown, AWS Account No. 3 also shares multiple common elements with both AWS Accounts No. 1 and No. 2. The registered name and email address for AWS Account No. 3, ROXANA COSTINA and ROXANACOSTINA@protonmail.com, are similar to those used by the other two accounts. In addition, AWS Account No. 3 shares the same billing address as both AWS Accounts No. 1 and No 2. Finally, AWS Account No. 3 includes debit card number 4256031149608984, which is also associated with AWS Account No. 1.

43. **Target Account No. 8** is the email address for AWS Account No. 8. AWS Account No. 8 includes debit card number 4256031180393017, which was associated with AWS Account No. 4. In addition, the phone number for AWS Account No. 8 was +40 727571425, which was also associated with AWS Account No. 3. Both AWS Accounts No. 3 and No. 4 can be linked to AWS Account No. 1, as shown in the preceding paragraphs.

The Target Accounts

44. During the course of this investigation and as described above, the Government identified the following email accounts (the "**Target Accounts**"):

- **lwestendtoys@gmail.com (Target Account No. 1)**
- **seller-performance@8cnzvfen-amazon.com (Target Account No. 2)**
- **seller-performance@2bv5bden-amazon.com (Target Account No. 3)**
- **seller-performance@1cr4x7en-amazon.com (Target Account No. 4)**
- **edelmira.salinas.ruiz@gmail.com (Target Account No. 5)**
- **mata82465@gmail.com (Target Account No. 6)**
- **detreaba112@gmail.com (Target Account No. 7)**
- **adypv1@gmail.com (Target Account No. 8)**

45. The requested information pertaining to the **Target Accounts** likely will provide additional information concerning the subjects' identities and whereabouts. In particular, data revealing the senders and recipients of emails to and from these accounts during the requested time period (January 1, 2020 through the present) would show whether the subjects used any of the above accounts to victimize additional Amazon sellers.

46. Each of the Target Accounts either was directly used in, or has a strong connection to this fraud scheme that has caused at least $529,834.90 in actual fraudulent disbursements and another $2,208,444.92 in attempted fraudulent disbursements. **Target Accounts No. 1-4** were actually used to email victims of the fraud scheme, and **Target Accounts No. 5-8** have strong connections (including the same or similar debit cards, card holder names, phone numbers, and/or billing addresses) to the AWS accounts that were used to perpetrate the fraud scheme.

BACKGROUND CONCERNING EMAIL

47. In my training and experience, I have learned that Google provides a variety of online services, including email access, to the public. Google allows subscribers to obtain email

accounts at the domain name Gmail.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail users) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

48. A Gmail user can also store files with the provider in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google.

49. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

50. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I

know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

51. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP addresses can help to identify which computers or devices were used to access the email account.

52. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

53. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the

disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.[1]

54. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can

---

[1] It is possible that Google stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 829 F.3d 197 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States—pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information sought is stored.

understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account owner's state of mind as it relates to the investigated offense. For example, information in the account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

55. Based on the foregoing, I respectfully submit that there is probable cause to believe that the email addresses described in Attachment A were used to further a criminal scheme or artifice to defraud, and I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Steele D. Holland

Steele Holland
Task Force Officer
Federal Bureau of Investigation

Reviewed and approved by AUSA Shea Gibbons

Sworn and attested to me by the Affiant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this date: April 14, 2021

/s/

Elizabeth W. Hanes
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information and documentation associated with

- **lwestendtoys@gmail.com,**
- **seller-performance@8cnzvfen-amazon.com,**
- **seller-performance@2bv5bden-amazon.com,**
- **seller-performance@1cr4x7en-amazon.com,**
- **edelmira.salinas.ruiz@gmail.com,**
- **mata82465@gmail.com,**
- **detreaba112@gmail.com, and**
- **adypv1@gmail.com**

that are stored at premises owned, maintained, controlled, or operated by Google Corporation, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, *regardless of whether such information is stored, held or maintained inside or outside of the United States*, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, device information, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including: full name, user identification number, birth date, gender,

contact email addresses, Google passwords, Google security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;

e. All records or other information pertaining to Google search history conducted by an individual using the account;

f. All records or other information containing historical location data maintained by Google associated with the account including GPS, Cellular, Wifi, or other in the custody or control of Google;

g. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

h. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

i. All "check ins" and other location information;

j. All documents, spreadsheets, photos or other files stored in Google Documents, Google Drive, or Google Photos

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C. §§ 1028A, 1029, 1030, 1343, 1349, and 1956 involving the individual(s) using the email addresses **lwestendtoys@gmail.com, seller-performance@8cnzvfen-amazon.com, seller-performance@2bv5bden-amazon.com, seller-**

performance@1cr4x7en-amazon.com, edelmira.salinas.ruiz@gmail.com, mata82465@gmail.com, detreaba112@gmail.com, and adypv1@gmail.com and occurring from the date of the account's opening, to include, for each account or identifier listed in **Attachment A**, information pertaining to the following matters:

a. Email communications and all content (intrinsic, embedded, or attached) related to fraud and related activity in connection with computers, Internet fraud schemes, any conspiracy to commit the aforementioned violations, or any other fraud activity. Communications between the email addresses **lwestendtoys@gmail.com, seller-performance@8cnzvfen-amazon.com, seller-performance@2bv5bden-amazon.com, seller-performance@1cr4x7en-amazon.com, edelmira.salinas.ruiz@gmail.com, mata82465@gmail.com, detreaba112@gmail.com, and adypv1@gmail.com** and any other individuals/accounts who may have wittingly or unwittingly played a role in assisting the scheme to defraud described above;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

e. The identity of any person(s) who have communicated with the target email address or shared documents or files about matters relating to money laundering and/or Internet fraud, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, and my official title is _____. I am a custodian of records for Google. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google; and

c. such records were made by Google as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature